Paul R. Kiesel, State Bar No. 119854
kiesel@kiesel.law
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel.: 310-854-4444
Fax: 310-854-0812

Barry. R. Eichen [Admitted *Pro Hac Vice*]
beichen@njadvocates.com
Evan J. Rosenberg [Admitted *Pro Hac Vice*]
erosenberg@njadvocates.com
Ashley A. Smith [Admitted *Pro Hac Vice*]
asmith@njadvocates.com
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Tel.: 732-777-0100
Fax: 732-248-8273

Stephen M. Gorny [Admitted *Pro Hac Vice*]
steve@gornylawfirm.com
Chris Dandurand [Admitted *Pro Hac Vice*]
chris@gornylawfirm.com
THE GORNY LAW FIRM, LC
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

Jay Barnes [Admitted *Pro Hac Vice*]
jaybarnes5@zoho.com
Rod Chapel [Admitted *Pro Hac Vice*]
rod.chapel@gmail.com
BARNES & ASSOCIATES
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

Attorneys for Plaintiffs

(Additional Attorneys Listed on Signature Page)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WINSTON SMITH; JANE DOE I; and JANE DOE II, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.; AMERICAN CANCER SOCIETY, INC.; AMERICAN SOCIETY OF CLINICAL ONCOLOGY, INC.; MELANOMA RESEARCH FOUNDATION; ADVENTIST HEALTH SYSTEM; BJC HEALTHCARE; CLEVELAND CLINIC; and UNIVERSITY OF TEXAS - MD ANDERSON CANCER CENTER,

Defendants.

CASE NO. 5:16-cv-01282-EJD

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Date: November 17, 2016
Time: 9:00 a.m.
Crtrm.: 4, 5th Floor
Judge: Hon. Edward J. Davila

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND CODES

RULES

TREATISES

I. INTRODUCTION

Privacy is not dead – not in sensitive health communications, not even on the Internet. Defendants' contentions to the contrary, the disclosure of personally-identifiable information ("PII") about persons communicating with health care providers over the Internet is not necessary for the Internet to function. The Mayo Clinic does not do it, nor does Johns Hopkins. The Defendants in this case do. That's what this case is about.

Far from "an attack on the way the Internet works," Plaintiffs instead seek to vindicate their constitutional, common law, and statutory rights to privacy in their sensitive medical communications with the health care Defendants who affirmatively (mis)represent that such communications are indeed private. In particular, this case is about: (1) the health care Defendants' websites' disclosure of sensitive medical communications to Facebook, in real-time, without the knowledge or consent of those with whom the Defendants are communicating (including their own patients), and in violation of their explicit privacy policies; and (2) Facebook's use of that sensitive information to sell targeted advertising.

Privacy is a fundamental right that finds its highest level of protection in medical information. *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998) ("One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health[.]"); *see also*, *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965) ("We deal with a right of privacy older than the Bill of Rights . . . .") Health privacy has also long been protected by the common law (*see DeMay v. Roberts*, 9 N.W. 146 (Mich. 1881)) and, in recent decades, by statute (*see, e.g.*, 42 U.S.C. § 1320d-6 (HIPAA); Cal. Civ. Code § 1798.91). In 2014, a unanimous Supreme Court held that Americans have a reasonable expectation of privacy in Internet medical communications – even when not made to a health care provider. *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("[C]ertain types of data are also qualitatively different. An Internet search and browsing history . . . could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

Facebook's self-serving argument to the contrary, general privacy principles still apply to the Internet. Although, as this Court has observed "this is an area of law that seems to be

developing," (*In re Facebook Internet Tracking Litig.*, Mot. to Dismiss Hr'g Tr. 17:12-13, Apr. 28, 2016) the trend is irrefutable – American courts in recent years have re-asserted and applied longstanding privacy rights to Internet communications – even outside the context of sensitive medical information. In *Google Cookie Placement*, the Third Circuit called defendants' argument that Internet tracking is "routine" and never highly offensive a "smokescreen" where the tracking at issue violated public privacy promises. 806 F.3d 125, 150 (3d Cir. 2015). Likewise, in *Nickelodeon Consumer Privacy Litig.*, the Third Circuit found plaintiffs adequately alleged a claim where the defendant "created an expectation of privacy on its websites and then obtained the plaintiffs' personal information under false pretenses." No. 15-1441, 2016 WL 3513782, at *22 (3d Cir. June 27, 2016). And in *Opperman v. Path*, the Court found that the unauthorized taking of consumer contact information was actionable, even over the defendants' objection that such behavior was "routine commercial behavior." 87 F. Supp. 3d 1018, 1058-61 (N.D. Cal. 2014).

Here, Defendants attempt a "universal defense"[1] to Internet privacy claims: if a company keeps its privacy policies vague but broad, nothing else matters – not their own promises, not legal prohibitions, and not sensitivity of information. According to Defendants, a broad statement buried in a privacy policy that no normal person ever reads (much less understands) creates immunity everywhere.[2] Taken to its logical conclusion, Facebook would be immune for its knowing receipt of, and profit from, hard copies of a person's complete medical file.

In effect, Facebook asserts obscure and vague privacy provisions operate as a blank check that must be read in isolation and trump any privacy policy on the health care Defendants' websites that expressly limits disclosure. Plaintiffs disagree and to find otherwise would be Orwellian. *See* George Orwell, *1984* 2 (1949) ("Big Brother is watching you . . . . The instrument (the telescreen, it

[1] *See In re: Facebook Internet Tracking Litig.*, Mot. to Dismiss Hr'g Tr. 30:7-9 ("THE COURT: It sounds like you're propounding a universal defense which is that's the way the Internet works, folks, and get over it.").

[2] *See Berkson v. GoGo, LLC*, 97 F. Supp. 3d 350, 381 (E.D.N.Y. 2015) (citing the comedian John Oliver, "If Apple put the entire text of Mein Kampf in their user agreement, you'd still click agree."); *see also Berkson* at 384 (citing a "[r]ecent empirical stud[y] analyzing the Internet browsing behavior of consumers" found that "between 0.05% and 0.22% of online shoppers access online agreements.").

was called) could be dimmed, but there was no way of shutting it off completely.").

Facebook and the health care Defendants are correct that the stakes are high. However, it is not the future of the Internet at stake but, rather, the future of Americans' fundamental right of privacy, which, once violated, can never be restored.

II. FACTUAL BACKGROUND AS ALLEGED[3]

The health care Defendants explicitly promise not to disclose PII to third-parties except in limited circumstances.[4] Facebook knows of these privacy promises.[5] The Plaintiffs sent and received sensitive medical communications with the health care Defendants.[6] However, in direct contravention of those privacy promises and without the knowledge or consent of the Plaintiffs, the health care Defendants disclosed PII about the Plaintiffs and details of their sensitive communications to Facebook in real-time.[7] What was promised to be kept private is no more. Significantly, disclosures to Facebook in violation of express privacy promises are not necessary to allow the health care Defendants' websites (or the Internet in general) to operate. In fact, Plaintiffs specifically alleged as much. Compl. ¶ 79 ("Facebook … does not track or intercept user

[3] As they have ignored the privacy of Plaintiffs and the Class, Defendants have also ignored that a Motion to Dismiss should address the allegations of the Complaint and no more. However, Defendants' Motion is replete with language that appears nowhere in the Complaint. *See, e.g.*, Mot. to Dismiss at 6:26–7:14 (touting, without citation, Defendants' reputations and work in a not-so-subtle attempt to excuse the conduct complained of).

[4] Compl. ¶¶ 107-12, Ex. F (Am. Cancer Soc.; "ACS"); 122-28, Ex. G (Am. Soc. of Clinical Oncology; "ASCO"); 137-43, Ex. H (Melanoma Research Foundation; "MRF"); 152-57, Ex. I (Adventist); 166-71, Ex. J (BJC); 181-84, Ex. K (Cleveland Clinic); 193-97, Ex. L (MD Anderson).

[5] Compl. ¶¶ 86-87, 129-31, 144-45, 158-59, 172-73, 185-86, 198-99, 222-24.

[6] Plaintiff Winston Smith sent and received communications relating to melanoma and cancer treatment. Compl. ¶¶ 117 (detailing communications with Cancer.org on treatment, insurance, support services, and lifestyle changes after cancer), 132 (detailing communications with Cancer.net on financing, treatment options, and emission tomography pet scans), 147 (detailing communications with Melanoma.org on baking soda treatment for melanoma), 202 (detailing communications with MDAnderson.org on metastatic melanoma). Plaintiff Jane Doe sent and received communications relating to pain management, treatment, and her doctor. Compl. ¶ 161 (detailing communications with ShawneeMission.org on pain management, orthopedic spine services, and Dr. Scott Ashcraft). Plaintiff Jane Doe II sent and received communications relating to a sensitive medical condition and her husband's doctor. Compl. ¶¶ 175 (detailing communications with BarnesJewish.org on her husband's doctor), 188 (detailing communications with ClevelandClinic.org on intestine transplants).

[7] Compl. ¶¶ 119-21 (ACS), 134-36 (ASCO), 149-51 (MRF), 163-65 (Adventist), 178-80 (BJC), 190-92 (Cleveland Clinic), 204-06 (MD Anderson).

communications with every website on which the Facebook icon appears. For example, … MayoClinic.org and … HopkinsMedicine.org include a small Facebook icon on nearly every page, but do not permit Facebook to track user communications. The same is true for hundreds if not thousands of other medical websites.").

Plaintiffs are members of Facebook who, like every other member, went through Facebook's sign-up process and agreed to its Terms, the first paragraph of which assures users:

> Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions. *Id.* at ¶ 60, Ex. A.

Despite underscoring that privacy is *very important* and promising to make *important disclosures*, Facebook fails to disclose that it tracks, collects, and intercepts user communications on sensitive health care websites in direct contravention of those websites' explicit privacy promises. *Id.* at ¶¶ 58-72. This interception occurs through the use of Facebook source code on web-pages controlled by the health care Defendants. As alleged, this code commandeers the Plaintiffs' web-browsers, permitting Facebook to acquire in real-time the communications connected to each user's IP address, browser fingerprint, and unique persistent Internet cookies assigned to each Facebook user and their particular browsers. *Id.* at ¶¶ 44-52.

Paragraph 50 illustrates how this works with an example of a communication between a user and Defendant ACS' Cancer.org website. *Id.* at ¶ 50a. First, the user sends the communication one of two ways – either by typing an entire URL into his web-browser toolbar, or by clicking on a hyperlink that contains information indicating it will send a communication on a particular topic – in this example, stomach cancer diagnosis. *Id.* at ¶ 50b. Regardless of whether the communication is sent manually by typing it into the toolbar or by a mouse click, the user has sent a communication to ACS about "stomach cancer diagnosis." *Id.* at ¶ 50c.

Immediately after the user hits Enter or clicks the mouse, the user's web-browser sends a GET request to ACS requesting information about stomach cancer diagnosis. *Id.* at ¶ 50d. However, unbeknownst to the user, the ACS webpage includes Facebook source code that directs the ACS web-server to commandeer the user's web-browser, ultimately commanding the browser to send a

separate but simultaneous GET request to Facebook attached to an exact duplicate of the user's communication to ACS. *Id.* at ¶ 50e. Without the user's knowledge, consent, or action, the web-browser follows commands from Facebook's source code, facilitating Facebook's real-time acquisition of (1) an exact copy of the communication the user sent to ACS, (2) cookie information that personally-identifies the user to Facebook, and (3) the user's IP address and device information, which also personally-identify the user to Facebook. *Id.* at ¶¶ 50f, 100-03. Facebook has acquired the communication and PII, but the communication between the user and ACS is still ongoing. *Id.* at ¶ 50f. ACS responds with a 2,535-word essay on stomach cancer diagnosis that does not finish loading until after Facebook acquired information about its substance. *Id.* at ¶ 50g.

In short, Facebook's code operates as an automatic routing program that permits Facebook to acquire exact duplicates of user communications, while they are still on-going, without the knowledge, consent, or any other action of the user. *Id.* at ¶ 52.

Much as it fails to disclose its activities to its users, Facebook also fails to disclose to web-developers that its source code as used by the health care Defendants will automatically result in Facebook's acquisition of communications.[8] *Id.* at ¶¶ 78, 84, Ex. D. After Facebook acquires the information, it uses it to sell advertisements targeted to users by medical conditions and interests including, but not limited to, lists such as "diabetes management," "chronic pain," "Hepatitis C," "bladder cancer," "rectal prolapse," and "diagnosis of HIV/AIDS." *Id.* at ¶¶ 88-91, Ex. E.

A. The Health Care Defendants' Privacy Policies

No reasonable person could read the health care Defendants' privacy promises and conclude that they disclose sensitive medical PII to Facebook in real-time.

American Cancer Society[9] – Defendants argue Cancer.org adequately informs users that it

[8] Without discovery, the plaintiffs cannot allege whether the health care Defendants knew about or consented to Facebook's acquisition of these sensitive communications in violation of their own privacy policies. *Id.* at ¶¶ 104-06.

[9] Cancer.org promises to "respect[] the privacy of every individual" who uses their websites. Comp. ¶ 109, Ex. F ("Because your privacy is important to us, we provide you with notice and choices about the collection and use of your information."). It next informs users that Cancer.org "use[s] cookies" but assures users that those cookies "do[] not contain any personal information." *Id.* at. Ex. F. It then promises that "Standard Web server traffic pattern information" on their websites "is shared externally only on an aggregated basis." *Id.* at. ¶ 110. ACS promises that user "health-related

discloses PII to Facebook via its advice to "read the privacy policies of each site you visit to determine what information that site may be collecting about you." Mot. to Dismiss 8:8-9. This is a non-sequitur – the PII disclosed by ACS is not occurring on another website, it is disclosed by ACS while the user is communicating with ACS. Defendants conveniently omit the rest of the paragraph:

> Our privacy policies apply only to your use of an ACS site. The www.cancer.org website contains links to other sites, including sites that have a special relationship with us. *We do not disclose personally identifiable information to those operating linked sites* and we are not responsible for their privacy practices. Links to other sites do not imply an endorsement of the materials or policies on those websites. You should read the privacy policies of each site you visit to determine what information that site may be collecting about you. Compl. Ex. F.

Thus, in addition to promising to only share traffic pattern information "on an aggregated basis," the very paragraph Defendants cite as notice includes another explicit promise: "We do not disclose personally identifiable information to those operating linked sites…." *Id.*

American Society of Clinical Oncology[10] – Defendants argue Plaintiffs are on notice of Cancer.net's PII disclosures to Facebook via a statement about "Click Stream Information." Mot. to Dismiss 8:1-7. Defendants again omit that the very sentence cited also refers to "Click Stream Information" as "NPI," defined one paragraph earlier as "anonymous Non-Personal Information." Compl. Ex. G § 4. As with Cancer.org, Defendants reference advice that users should "review the privacy policies of other sites carefully," but conveniently omit the rest of the paragraph. *Id*. at Ex. G. § 3 ("ASCO has also provided external links to other websites in order to provide those who use the Website with a better, more fulfilling experience. *Once you enter another website* … be aware that ASCO is not responsible for the privacy practices of other sites …. We encourage you to …

---

information is privileged and confidential and will not be shared or released to any organization or business entity other than those affiliated with or working in conjunction with ACS" as provided in specific examples. *Id.* at. ¶ 111, Ex. F.

[10] Cancer.net promises to "respect[] your privacy" and to be "committed to being transparent about how and when ASCO collects, uses, and safeguards the information we collect through our websites." Compl. Ex. G at 1. It then promises to tell users, among other things, "*who* collects information," "*what* information is collected and how this is done," and "*how* ASCO … discloses the information that is collected." *Id*. at Ex. G at 2. Despite this promise, ASCO does not disclose the *who* (the policy does not mention any relationship with Facebook), the *what* (it does not disclose the information Facebook collects), or the *how* (no mention of how it discloses information to Facebook). Instead, it promise to "only disclose your PII to third-parties" under a discrete list of seven circumstances, none of which were cited by Defendants or apply in this case.

review the privacy statements of each and every website that you visit through a link or sponsorship notice[.]") (emphasis added). Again, the disclosures are not happening on "another website" but rather this Defendant's own site.

Melanoma Research Foundation[11] – Defendants argue Plaintiffs are on notice of MRF's PII disclosures via a statement that "[m]any third-party sites have their own privacy policies that differ from ours." Mot. to Dismiss 8:10-11. Once again, Defendants omit the context:

> Our Service contains links to Internet sites maintained by third parties. These links are provided for your reference only. We do not control, operate or endorse in any respect information, products, or services on such third-party sites and are not responsible for their content. Many third-party sites have their own privacy policies that differ from ours. This Privacy Policy only covers our Service and does not cover any other site. Compl. Ex. H at ¶ 6.3.

Adventist[12] – Defendants argue Plaintiffs are on notice of Adventists' PII disclosures to Facebook via the "Links" section of its privacy policies. Mot. to Dismiss 8:11-13. Yet again, Defendants omit context:

> Our website may contain links to other sites. These links are for your convenience only, and Adventist Health System makes no representations or endorsements whatsoever regarding such other sites. You should review the privacy policies of other sites carefully before providing any information to such website. Adventist Health System is not responsible for the privacy policies or procedures or the content of any other website. Compl. Ex. I.

BJC Healthcare – Defendants argue Plaintiffs are on notice of PII disclosures to Facebook via a vague statement that "[i]nformation you submit may be routinely shared with … organizations working on [BJC's] behalf." Mot. to Dismiss 8:13-14. Again, Defendants omit the full context:

> A typical visit to our Web site does not require a user to submit personal information. However, if you decide to send us an email, respond to a survey, or subscribe to an online publication with your contact information, we will respond to you with the information you request and other information that we think might be of interest to you.…
>
> Information you submit may be routinely shared with our parent organization, BJC HealthCare as they often distribute our materials, or with the Washington University School of Medicine if you are looking for a physician referral. Other than these two organizations, we will only forward your personal information to

[11] MRF promises it does not "sell or share your Personal Data [defined as data that allows someone to identify or contact you] with Third Party Companies." Compl. Ex. H at ¶ 6.2.

[12] Adventist promises, "As a general rule, we will not disclose your personally identifiable information to any unaffiliated third party, except when we have your permission or under special circumstances[.]" Compl. Ex. I.

> organizations working on our behalf. We urge you not to provide any confidential information about you or your health to us via electronic communication. If you do so, it is at your own risk. Although we attempt to maintain our computer network in a secure manner to protect the content of your messages, we cannot provide absolute assurance that the contents of your email will not become accessible to individuals or entities that are not authorized to access your information. Compl. Ex. J at 2.

Thus, the language about "routine sharing" is limited to BJC itself and Washington University. Further, BJC's warning "not to provide any confidential information" is in the context of a disclaimer that BJC "cannot provide absolute assurance that the contents of your email will not become accessible" to unauthorized persons. Finally, Defendants' citation to a disclosure about BJC's own first-party cookies is completely irrelevant. First-party cookies are not at issue in this case.[13]

Cleveland Clinic[14] – Defendants argue Plaintiffs are on notice of Cleveland Clinic's PII disclosures to Facebook via statements about first-party cookies and disclaimers about site security. Mot. to Dismiss 8:18-20. Defendants' reference to first-party cookies is not relevant. Nor is the disclaimer. Defendants have again taken a sentence out of context. Just before the disclaimer, Cleveland Clinic provides the preface that, "[B]y its very nature, a website cannot be absolutely protected against intentional or malicious intrusion attempts." Compl. Ex. K at 2. While perhaps true, this Defendant could absolutely have taken steps to avoid the disclosure complained of here. Cleveland Clinic further professes that it will take "reasonable care to safeguard your information while in transit[.]" *Id*. at Ex. K at 3.

MD Anderson[15] – MD Anderson bases its defense solely on the Eleventh Amendment.

---

[13] Defendants neglect to mention that BarnesJewish.org does not maintain a clearly marked "Privacy Policy" link on its homepage. Instead, the bottom of each page includes a link to a "HIPAA" page, which assures users, "We are required by law to protect the privacy of your protected health information" and defines PHI to include "information that [BJC] create[s] or receive[s] that identifies you and your past, present or future health status or care[.]" Compl. ¶ 169, Ex. J. The Privacy Policy is only accessible through a link that states "Legal."

[14] ClevelandClinic.org promises, "Cleveland Clinic does not share any [PII] of any individual with any third party unrelated to Cleveland Clinic, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization."

[15] MD Anderson promises, "Under no circumstances will we ever disclose (to a third party) personal information about individual medical conditions or interests, except when we believe in good faith that the law requires it." Compl. ¶197, Ex. L.

III. LEGAL STANDARDS

On a 12(b)(6) motion to dismiss, the Court must "accept factual allegations in the Complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine, Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). To survive, the complaint need only allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Dismissal is only appropriate "where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008).

IV. ARGUMENT

A. Plaintiffs Have Standing to Bring this Action

To establish standing under Article III, a plaintiff must allege that "he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Spokeo v. Robins*, 136 S. Ct. 1540, 1548 (2016).[16] "Concrete" is not synonymous with tangible and such harm may arise from a statutory violation. *Id.* at 1549 (citing cases involving fundamental rights to freedom of speech and religion as "intangible injuries" that "can nevertheless be concrete" and re-affirming that "Congress may elevate to the status of legally cognizable injuries, de facto injuries that were previously inadequate in law"). In such cases, *Spokeo* explains that a "right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified." *Id.*

1. Plaintiffs Allege Sufficient Privacy Harm

Where an alleged injury is intangible, *Spokeo* instructs courts to make two inquiries. First,

[16] Plaintiffs plead "particularized" injury. *See* Compl. ¶¶ 117, 132, 147, 161, 175, 188, 202.

"courts should consider 'whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing the basis for a lawsuit in English or American courts.'" *Mey v. Got Warranty*, No. 15-cv-00101-JPB-JES, 2016 WL 3645195 at *5 (N.D. W. Va. June 30, 2016) (citing *Spokeo*, 136 S. Ct. at 1548). "Second, Congress may 'elevate to the status of legally cognizable injuries that were previously inadequate at law.…' It 'has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before.'" *Id.* at *6.

This case satisfies both inquiries: first, it involves the right to privacy, described by the Supreme Court as "a most fundamental human right" enshrined in the "specific guarantees in the Bill of Rights," "older than the Bill of Rights," and "the most comprehensive of rights and the right most valued by civilized men." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 487 (1974); *Griswold*, 381 U.S. at 484; *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *accord*, *Berger v. New York*, 388 U.S. 41 (1967), citing 4 Blackstone Commentaries 168 (1765) and *Entick v. Carrington*, 19 How. St. Tr. 1029, 1066 (1765) ("Intrusions into privacy are 'subversive of all the comforts of society.'"). More specifically, privacy of a particularly sensitive sub-set of information invokes the highest standards of protection. *Norman-Bloodsaw* at 1269 ("One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health"). Since at least 1881, Americans have had standing to sue violators of their medical privacy even in the absence of economic harm. *See DeMay*, 9 N.W. at 146.

Post-*Spokeo* courts have found adequate standing allegations in privacy cases involving rights to privacy in information less substantial than medical communications. *See Bona Fide Conglomerate v. SourceAmerica*, No. 14-cv-00751-GPC-DHB, 2014 WL 4162020 (S.D. Cal. June 29, 2016) (stating that alleged violations of California Invasion of Privacy Act [also alleged in this case] satisfy *Spokeo*); *In re: Nickelodeon Privacy*, 2016 WL 3513782 at *6-8 (3d Cir. June 27, 2016) (finding standing based on alleged tracking and disclosure of minors' private personal information at the defendant's children's websites); *Mey v. Got Warranty*, Order Denying Defendants' Motion to Dismiss (finding standing under the Telephone Consumer Protection Act based on common law history of right to privacy and Congressional purposes in enacting the

TCPA).[17]

Second, this case involves precisely the type of harm Congress intended to prevent with the passage of the Electronic Communications Privacy Act of 1986. S. Rep. No. 99-541, at 5 (1986). "[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment . . . Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right . . . ." *Accord*, H.R. Rep. No. 99-647, at 19 (1986).

2. Plaintiffs Allege Sufficient Economic Harm

In addition to intangible but legally concrete privacy harm, Plaintiffs allege a robust market for the sensitive medical information wrongfully disclosed and tracked. Compl. ¶¶ 53-57 (describing "Value of the Personal Information Defendants Collect"), 88-91 (explaining how Facebook monetizes data wrongfully collected). This is enough. As Judge Koh recently explained in another medical privacy case, "Plaintiffs are not required to plead that there was a market for their PII and that they somehow also intended to sell their own PII." *In re: Anthem Data Breach Litig.*, No. 15-md-02617-LHK (N.D. Cal. May 27, 2016), Order Granting in Part and Denying in Part Defendants' Second Mot. to Dismiss, at *27. Instead, it is enough to allege "either an economic market for their PII or that it would be harder to sell their own PII, not both." *Id.* Likewise, Plaintiffs alleged "Benefit of the Bargain Losses" for Facebook's Breach of Fiduciary Duty of Good Faith and Fair Dealing. Compl. ¶ 362.

B. This Court Has Jurisdiction Over All of the Health Care Defendants

1. The Court's Exercise of Personal Jurisdiction Is Proper

A plaintiff need only make a prima facie showing of personal jurisdiction to withstand a motion to dismiss under Rule 12(b)(2). *Mattel, Inc. v. Greiner & Hausser GmbH*, 354 F.3d 857,

[17] Two cases cited by Defendant are inapposite. First, *Khan v. Children's National Health System* did not deal with the question of federal statutory standing as it involved plaintiffs' invocation of state-only data breach statutes in federal court. 2016 WL 2946165 (D. Md. May 19, 2016). Similarly, in *Gubala v. Time Warner*, plaintiffs alleged unlawful retention of information, not its unlawful collection or disclosure. 2016 WL 3390415 (E.D. Wis. June 17, 2016).

862 (9th Cir. 2003). Plaintiffs have alleged sufficient facts to support this Court's exercise of general and specific personal jurisdiction over the health care Defendants.

General Jurisdiction – A court may exercise general jurisdiction over foreign corporations to hear any and all claims against them when their affiliations with the State are so continuous and systematic as to render them essentially at home in the forum State. *Daimler AG v. Bauman*, 134 S. Ct. 746, 754 (2014). Contrary to Defendants' contention, the health care Defendants' affiliations with California are indisputably consistent and systematic and consist of significantly more than just operating a website. Indeed, the health care Defendants continuously and systematically send users' sensitive medical communications to Facebook, which is headquartered in California, each and every time a user sends a GET request to the health care Defendants' respective websites. Such activity is not random or fortuitous. It is nothing less than continuous and systematic, thereby rendering them essentially at home in California and subject to this Court's general jurisdiction.

Specific Jurisdiction – A defendant is subject to specific jurisdiction if (1) it purposefully directed its activities to the forum or purposefully availed itself of the privilege of conducting activities in the forum, (2) the plaintiff's claim arises out of the defendant's forum-related activities, and (3) the exercise of jurisdiction comports with fair play and substantial justice, that is, it is reasonable. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004).

Here, all three prongs of the specific jurisdiction test are satisfied. First, the health care Defendants purposefully directed their activities to California. That Plaintiffs do not reside in California is not fatal. *See Walden v. Fiore*, 134 S. Ct. 1115, 1122 (2014). As explained above, the health care Defendants send users' sensitive medical communications to Facebook every time a user sends a GET request to the health care Defendants' respective websites. Additionally, such Defendants seemingly concede that their conduct is purposeful in that, in their Motion, they contend that their respective websites sufficiently disclosed such conduct. Mot. to Dismiss 7:20-26, 18:5-13.

Second, Plaintiffs' claims clearly arise out of the health care Defendants' California-related activities. Namely, Plaintiffs' claims arise out of, in substantial part, the health care Defendants' sending Plaintiffs' sensitive medical communications to Facebook in real-time, without Plaintiffs' knowledge or consent, and in violation of the health care Defendants' explicit privacy promises.

Third, this Court's exercise of jurisdiction over the health care Defendants comports with fair play and substantial justice. The fulcrum of activity in this action is with Facebook. The health care Defendants' relevant conduct occurred in California. Additionally, pursuant to Facebook's Terms of Service, Facebook users, including web developers and operators like the health care Defendants, submit to this Court's personal jurisdiction for the purpose of litigating all claims related to Facebook. Compl. Ex. A at 4. This Court is the single most reasonable court in which Plaintiffs could bring this action against the health care Defendants.

ACS's argument that its Georgia forum selection clause prevents this Court from exercising personal jurisdiction over it is also without merit. To the contrary, each health care Defendant, including ACS, is subject to Facebook's forum selection clause and this Court's jurisdiction since non-parties can be held to forum selection clauses if the conduct of the non-parties is closely related to the contractual relationship. *Manetti-Farrow, Inc. v. Gucci America, Inc.*, 858 F.2d 509, 514 n.5 (9th Cir. 1988); *Holland Am. Line, Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 456 (9th Cir. 2007). The health care Defendants' relevant conduct is inextricably related to the relationship between Plaintiffs and Facebook. Moreover, this claim stems from users like Plaintiffs being Facebook members and the health care Defendants being users of Facebook code. The health care Defendants, therefore, are subject to Facebook's forum selection clause and this Court's jurisdiction.

2. MD Anderson Is Not Immune from Suit

Under the Full Faith and Credit Clause, the law demands application of California's typical rules of immunity and California's immunity-related statutes. *See Franchise Tax Bd. of Cal. v. Hyatt*, 136 S. Ct. 1277, 1281-82 (2016); *Nevada v. Hall*, 440 U.S. 410, 424 (1979) (California court may apply California sovereign immunity law to State of Nevada). MD Anderson may only rely on sovereign immunity, if at all, to the extent consistent with California law. *Hyatt*, 136 S. Ct. at 1281-82. The California state-law claims should not be dismissed as the allegations are sufficient to state claims against MD Anderson under California law. Further, as discussed above, MD Anderson, by using Facebook's code, affirmatively consented to California law and chose California as the venue for disputes. Additionally, the Wiretap Act permits an aggrieved party to sue "the person *or entity*, other than the United States, which engaged in that violation." 18 U.S.C. § 2520(a) (emphasis

added). *Seitz v. City of Elgin* explicitly forecloses Defendants' argument: "the plain meaning of 'entity' includes government units." 719 F.3d 654, 657 (7th Cir. 2013). Thus, any purported sovereign immunity is explicitly waived in the Wiretap Act. 18 U.S.C. § 2520(a).

C. Plaintiffs' Claims Survive Dismissal

1. Plaintiffs Did Not Consent to the Harm Complained of

Defendants bear the burden of proving the affirmative defense of consent. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003). However, as consent does not appear in the Complaint, it should not be resolved on Facebook's 12(b)(6) motion. *Scott v. Kuhlmann*, 746 F.2d 1377-78 (9th Cir. 1984) (citing Wright & Miller, Federal Practice and Procedure § 1277 at 328-30) (affirmative defenses ordinarily may not be raised in motion to dismiss unless there are no disputed issues of fact); *Conway v. Geithner*, No. C-12-0264, 2012 WL 1657156 at *2 (N.D. Cal. 2012). Accordingly, Defendants have not carried their burden.

a. Consent for Sensitive Medical Information Must Be Express, Knowing, and Written

This is not a case about the disclosure of ordinary information, but instead sensitive medical information, which is afforded the highest degree of constitutional, common law, and statutory protection from tracking and disclosure. Compl. ¶ 216b ("The Plaintiffs' communications with Adventist, BJC, Cleveland Clinic, and MD Anderson related to their 'past, present, and future physical or mental health or condition.'"). To rule on this Motion, this Court will necessarily have to apply a test to determine whether the Defendants' disclosures were adequate and that Plaintiffs consented to the challenged activity. The proper tests for tracking and disclosure of sensitive medical information are found in HIPAA and California Civil Code section 1798.91. Under these tests (or as detailed below, the test urged by Defendants), Plaintiffs have not consented.

HIPAA – Disclosure and receipt of medical information requires express, knowing, and written consent. "A person who knowingly and in violation of [HIPAA] – (1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section." 42 U.S.C. § 1320d-6(a). "[A] person . . .

shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization." *Id.*

Defendants Adventist, BJC, Cleveland Clinic, and MD Anderson are "covered entities" under HIPAA. Defendants argue, however, that they are only "covered entities" when engaged in "specific transactions." Mot. to Dismiss 28:13-29:3. This argument is at odds with the plain language of 42 U.S.C. § 1320d-6(a) cited above, as well as the regulations enforcing HIPAA. Under 45 C.F.R. § 164.502, a "covered entity … may not use or disclose protected health information, except as permitted or required [by HIPAA]." This requirement is not limited to the instances when a covered entity is engaged in one of the "specific transactions" cited by Defendants. For example, covered entities were found to violate HIPAA by (1) leaving a telephone message on a patient's answering machine,[18] and (2) responding to a subpoena without making reasonable efforts to ensure that the individual whose PII was sought had received notice of the request.[19] Neither of these HIPAA violations involved one of the "specific transactions" referenced by Defendants.

In addition, "protected health information," by the plain language of the Privacy Rule, is not limited to patients of a covered entity. Instead, "health information" is defined as "any information … whether oral or recorded in any form or medium that … (1) is created or received by a health care provider … and (2) [r]elates to the past, present, or future physical or mental health or condition of an individual." 45 C.F.R. § 160.103. "Health information" becomes "protected" under HIPAA when it is "individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form of media." 45

[18] "Large Provider Revises Contact Process to Reflect Requests for Confidential Communications," U.S. Department of Health & Human Services, Health Information Privacy, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html#case2; "Hospital Implements New Minimum Necessary Policies for Telephone Messages," U.S. Department of Health & Human Services, Health Information Privacy, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html#case26.

[19] "Public Hospital Corrects Impermissible Disclosure of PHI in Response to a Subpoena," U.S. Department of Health & Human Services, Health Information Privacy, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html#case9.

C.F.R. § 160.103. In turn, information is considered "individually identifiable" under HIPAA unless it has been scrubbed of all "identifiers of the individual *or* of *relatives*, employers, or *household members* of the individual." 45 C.F.R. § 164.514(b)(2) (emphasis added). These "identifiers" include names, geographic subdivisions smaller than a state, device identifiers and serial numbers, IP addresses, and any other unique identifying numbers, characteristics or code tied to "the individual" or their "relatives, employers, or household members." 45 C.F.R. § 164.514(b)(2).

Information considered PII may only be disclosed with proper HIPAA authorization on a signed document containing (1) "specific and meaningful" disclosures of the information to be disclosed, (2) the persons to whom it will be disclosed, a description of the information to be disclosed, (3) an expiration date for disclosure, and (4) notice of the right to revoke authorization. Compl. ¶ 212. The covered entity must also write its authorization in plain language and provide the individual with a signed copy. *Id.*

In this case, the Plaintiffs' communications are protected by HIPAA. The communications at issue were recorded and received by health care providers. *Id.* at ¶ 215 ("the covered entity websites each tracked, created, and recorded logs of the Plaintiffs' activities on the health care websites through the websites' own use of cookies and other [PII] including, but not limited to, device identifiers and IP addresses."). These communications relate to the Plaintiffs' "past, present, or future physical or mental health or conditions," or, in the case of Jane Doe II, her spouse. *Id.* at ¶¶ 216b ("The Plaintiffs' communications with Adventist, BJC, Cleveland Clinic, and MD Anderson related to their 'past, present, and future physical or mental health or condition.'"), 161 ("Plaintiff Jane Doe sought information … relating to pain management and her particular doctor."), 175 ("Plaintiff Jane Doe II sought information … relating to a sensitive medical condition, and her husband's doctor.").[20] The communications were disclosed to Facebook connected to information deemed individually-identifiable under 45 C.F.R. § 164.514(b)(2). *Id.* at

[20] To the extent necessary, Plaintiffs will if given leave, file an amended complaint alleging that Plaintiff Winston Smith was also seeking information and engaging in communications relating to his own "past, present, and future physical or mental health or conditions."

¶¶ 82 (describing Facebook cookies), 99-103 (describing why even non-cookie information (IP addresses and device identifiers) are personally identifiable to Facebook), 220. Finally, the covered entities disclosed the information to Facebook in the absence of a valid HIPAA authorization – and, in fact, in direct violation of their own privacy policies. *Id.* at ¶ 221.

Cal. Civ. Code § 1798.91 – California law provides that "[a] business may not request in writing medical information directly from an individual regardless of whether the information pertains to the individual or not, and use, share or otherwise disclose that information for direct marketing purposes" unless it first "disclose[s] in a clear and conspicuous manner that it is obtaining the information to market or advertise products, goods, or services to the individual" and "obtain[s] the written consent of the individual to whom the information pertains … to permit his or her medical information to be used or shared to market or advertise products, goods, or services to the individual." Cal. Civ. Code § 1798.91. Facebook is a business engaged in direct marketing. Compl. ¶¶ 227-28. Plaintiffs' communications qualify as "medical information" under this section. *Id.* at ¶ 230. Facebook's disclosures were not "clear and conspicuous." *Id.* at ¶¶ 233-34.

b. ECPA Consent Must Be "Actual" and Not "Casually Inferred"

For ECPA claims, "consent should not casually be inferred." *Pharmatrak* at 20. "Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception." *Id*. "Consent may be explicit or implied, but it must be actual consent rather than constructive consent." *Id*. at 19. It involves a two-part inquiry. First, a court must determine the "dimensions of the consent." *Id*. Then, it must ascertain "whether the interception exceeded those boundaries." *Id.*[21]

In *Pharmatrak*, the defendant was a third-party cookie company whose source code was voluntarily placed onto the websites of health care (pharmaceutical) companies. Even though the health care websites placed Pharmatrak code on their webpages, they did not know of or consent to the extent of the information Pharmatrak acquired. The Court found the plaintiffs provided adequate

[21] This analysis is no different in the Internet context than in any other. A medical patient may consent to one treatment (a physical exam), but refuse another (colonoscopy). A landowner may consent to one trespass (bird-watching), but not another (duck hunting).

evidence to assert an ECPA claim. As in *Pharmatrak*, this case involves third-party cookies utilized through source code on a health care company's website. And, each health care Defendant explicitly promised not to disclose certain information to Facebook, even though it did (discovery will reveal the extent of the health care Defendants' knowledge of and consent to Facebook's activities). Further, "[t]he existence of implied consent is a question of fact[.]" *Konop v. Hawaiian Airlines, Inc*., 236 F.3d 1035, 1047-48 (9th Cir. 2001) (citing *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990) ("The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of [the Wiretap Act] – a purpose which suggests that consent should not casually be inferred.")).

Defendants assert that the test for consent in this case is: "Would a reasonable user who viewed [the defendants'] disclosures have understood that [Facebook] was collecting [the information at issue]?" Mot. to Dismiss 16:7-8, citing *Perkins v. LinkedIn Corp*., 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014). But, in light of HIPAA and California Civil Code section 1798.91's greater protections for sensitive medical information, this misstates the question. It also leaves out half of the equation: would a reasonable user have understood that the health care Defendants were disclosing personally identifiable information about them to Facebook even though their privacy policies explicitly promised not to share such information?

Regardless, even under Defendants' test, a reasonable user would not have understood that the health care Defendants were violating their own privacy policies. *Perkins* explains why. There, LinkedIn's disclosure "was not, as is often the case, … buried in a Terms of Service or Privacy Policy that may never be viewed or if viewed at all on a wholly separate page disconnected from the processes that led to the alleged wrongful conduct." *Perkins*, 53 F. Supp. 3d at 1212. "Even more significantly, perhaps," *Perkins* explains, "is the fact that alongside the disclosure is an express opt out opportunity in the form of the 'No thanks' button." *Id. Perkins* determined it was only "[i]n light of the clarity of the disclosure, the proximity of the disclosure to the wrongful conduct, and the ability to opt out" that the LinkedIn plaintiffs consented to and authorized the

collection of email contacts. *Id.* Here, however, (1) the health care Defendant explicitly promised not to disclose PII, Facebook failed to disclose that it collects PII in this way, and any Facebook disclosures were vague and contained in a Privacy Policy "on a wholly separate page;" (2) the wrongful conduct occurred on the webpages of health care Defendants far away from the vague disclosure "buried in a Terms of Service or Privacy Policy that may never be viewed;" and (3) Facebook users do not have the option to opt-out of Facebook's tracking of this medical information.

Review of the health care Defendants' privacy policies in light of the particular sections cited in the Motion demonstrates that no reasonable person would have understood that their websites were disclosing PII to Facebook. As explained above, Defendants offer a series of non-sequiturs regarding the explicit promises made by the health care Defendants. Further, Facebook's Statement of Rights and Responsibilities ("SRR") combined with its Data Use Policy cannot be said to apprise reasonable persons that Facebook would track their sensitive medical communications with websites that explicitly promise not to make such disclosures. Again, Facebook's SRR begins by promising users, "Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information." Compl. ¶ 60, Ex. A ¶ 1 (emphasis added). Is a disclosure that Facebook tracks, records, and intercepts sensitive medical communications that its users make on health care websites' (including HIPAA-covered entities) that explicitly promise not to disclose the contents of those communications *important*? A reasonable person would believe it was, and yet Facebook made no such disclosure.

To the extent Facebook has disclosed anything with regard to its tracking and acquisition of communications, applying those disclosures to communications the Plaintiffs exchanged with the health care Defendants in this case would render Facebook's SRR and Data Use Policy unenforceable and unconscionable. Defendants argue these vague but broad terms create a universal defense to all privacy actions. Yet, just as ordinary privacy and consent principles apply to the Internet, so too do ordinary contract principles. *See Specht v. Netscape*, 306 F.3d 17, 30 (2d Cir. 2002) (J. Sotomayor) (interpreting California contract law as it applied to Internet Terms of Use,

"California's common law is clear that 'an offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious."); *Berkson*, 97 F. Supp. 3d at 404 (discussing procedural and substantive unconscionability in Internet contracts of adhesion, citing Restatement (Second) of Contracts § 211(3), where the offering party has reason to believe "that the party manifesting assent" to a contract "would not do so" if she "knew that the writing contained a particular term, the term is not part of the agreement"); *Mastrobuono v. Shearson Lehman Hutton, Inc.*, 514 U.S. 52, 63 (1995) ("As a practical matter, it seems unlikely that petitioners … had any idea that by signing a standard-form agreement to arbitrate disputes they might be giving up an important substantive right. In the face of such doubt, we are unwilling to impute this intent to petitioners.").

2. The Wiretap Act Claim Is Proper

Interception – The ECPA defines "intercept" as the "acquisition of the contents of any … electronic communication[.]" Federal courts have squarely rejected Facebook's argument that the acquisition must be made via the same communication. In language directly on point, the First Circuit rejected an identical argument with respect to a third-party cookie defendant's acquisition of the content of sensitive medical information on health care websites:

> Even those courts that narrowly read 'interception' would find that Pharmatrak's acquisition was an interception. … NETcompare was effectively an automatic routing program. It was code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third-party (Pharmatrak).
>
> Pharmatrak argues that there was no interception because 'there were always two separate communications: one between the Web user and the Pharmaceutical Client, and the other between the Web user and Pharmatrak.' This argument fails
>
> for two reasons. First, as a matter of law, even the circuits adopting a narrow reading of the Wiretap Act merely require that the acquisition occur at the same time as the transmission; they do not require that the acquisition somehow constitute the same communication as the transmission. Second, Pharmatrak acquired the same URL query string (sometimes containing personal information) exchanged as part of the communication between the pharmaceutical client and the user. Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement.

In re: Pharmatrak, 329 F.3d at 22; *see also U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010)

(email forwarding).

Facebook also attempts to shoehorn the Wiretap Act's exception for a "party to the communication" into its "interception" defense. However, as this Court has previously held, Facebook cannot claim the "party" exemption simply because a "Facebook server was involved" when there is nothing to "demonstrate that Plaintiffs knew that fact while their browsing activity was being tracked and collected." *In re: Facebook Internet Tracking Litig.*, Order Granting Def.'s Mot. to Dismiss at 18. Also, Defendants' reliance upon the "party to the communication" rule stated in *Google* and *Nickelodeon* is misplaced. In *U.S. v. Eady*, decided in the five months between those cases, the Third Circuit adopted a different rule, defining "party to the communication" as "an individual who participates with at least one other individual in a communication and whose participation in that communication is known to the other participant(s) in the communication at the time of the communication." 2016 WL 2343212 (3d Cir. May 4, 2016) (unpublished opinion). As the *Eady* panel explained, "a defendant does not actually participate in a conversation unless his presence is known to the other participants." *Id*. at *3.

In this case, Plaintiffs did not know Facebook was acquiring the communications they were exchanging with the health care Defendants. And, as set out above, the health care Defendants explicitly promised the opposite. In addition, Facebook did not disclose to its users that it acquires their communications with the health care Defendants nor that it acquires communications in violation of other websites' privacy policies or federal and state medical and other privacy laws.

Content – Under the Wiretap Act, content "includes any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The Complaint details 15 instances in which Facebook acquired information concerning the substance, purport, or meaning of a communication. Compl. ¶¶ 117, 132, 147, 161, 175, 188, 202, 269. For example, Facebook acquired communications between Winston Smith and MD Anderson relating to "Metastatic Melanoma" via: http://www2.mdanderson.org/cancerwise/2012/06/metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnosis.html. Id. at ¶¶ 202, 269(g). The phrase "metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnosis" includes information concerning the "substance, purport, and meaning" of the communications between Winston Smith

and MD Anderson. Arguments to the contrary are absurd.

No court has ever ruled that URLs as specific as these are not protected by the Wiretap Act. In *Zynga*, the Ninth Circuit explained that URLs contain content where they include "search term[s] or similar communication[s] made by the user[.]" *In re: Zynga Privacy*, 750 F.3d 1098, 1109 (9th Cir. 2014). In *Google Cookie*, the Third Circuit explained "post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user … between the information revealed by highly detailed URLs and their functional parallels to post-cut-through digits, we are persuaded that – at a minimum – some queried URLs qualify as content." *In re: Google Cookie Placement*, 806 F.3d at 139. As this Court has noted, the *Google Cookie* Court's "analysis of this type of communication" was "very thorough … impressive … and very thoughtful" and what *Google Cookie* "tells us [is] that there are other circumstances when you drill down, not necessarily that deep, that you can find that the URLs have actual content and ours could be offensive in some manner." *See In re: Facebook Internet Tracking Litig.*, Mot. to Dismiss Hr'g Tr. 17-18.

This is one of those circumstances. Case law, legislative history, and logic on this point overwhelmingly support the Plaintiffs. *See U.S. v. Forrester*, 512 F.3d 500, n.6 (9th Cir. 2008) (URLs, unlike mere IP addresses, "reveal[] much more information" about user's activity, including articles viewed); *Declassified Opinion from the FISC*, https://www.dni.gov/files/documents/1118 CLEANEDPRTT%202.pdf (content and DRAS under ECPA not mutually exclusive); *In re: Application for Pen Register*, 396 F. Supp. 2d 45, 49-50 (D. Mass. 2005) ("Contents" include URL "subject lines, application commands, search queries, requested file names, and file paths); *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000) (post-dialed digits); *Brown v. Waddell*, 50 F.3d 285, 87-88 (4th Cir. 1995); *In re: Pharmatrak*, 329 F.3d at 18; H.R. Rep. 107-236, at 53, 294-96 (2001) (legislative history to PATRIOT ACT, explaining a pen register order "could not be used to collect information other than [DRAS], such as the portion of a URL specifying Web search terms or the name of a requested file or article" and that, according to Rep. Zoe Lofgren (D-San Jose), "in the discussions that we had … with the Justice Department and the White House, they made it very clear that they agreed with this, and this is not an agreement. It is just a clarification,

and I think that is important for the public to know[.])[22]

Device – The ECPA defines an "electronic … or *other* device" as "*any* device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). "Other" and "any" focus the ECPA definition on function – *i.e.*, whether something can be used to intercept (acquire) communications. Congress chose broad definitions to further the central purpose of the Wiretap Act – "to protect effectively the privacy of … communications." *Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001). The dictionary definition of device includes, among other things, (1) "a thing made for a particular purpose; an invention or contrivance"; (2) "a plan or scheme for effecting a purpose," and (3) "a crafty scheme, trick." http://www.dictionary.com/browse/device.

Plaintiffs allege seven different devices: (1) cookies and other tools used by Facebook to track Plaintiffs' communications; (2) the Plaintiffs' web-browsers; (3) the Plaintiffs' computing devices; (4) Facebook's web servers; (5) the web servers of the health care Defendants; (6) the source code deployed by Facebook to effectuate its acquisition of communications; and (7) the plan Facebook carried out to effectuate the acquisition of information in this case. Compl. ¶ 261; *see also Id*. at ¶ 50 (describing how these devices work together to effectuate Facebook's scheme).

Web servers and computers are devices under the ECPA.[23] *Szymuszkiewicz*, 622 F.3d at 707 (discussing *Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001)). Software and computer code are devices. *In re: Carrier IQ, Inc., Consumer Privacy Litig.*, 78 F. Supp. 3d 1051, 1067 (N.D. Cal. 2015). Facebook's cookies are ECPA devices because they are an invention

---

[22] The full report is available online through the United States Government Printing Office. *See* https://www.congress.gov/107/crpt/hrpt236/CRPT-107hrpt236-pt1.pdf

[23] *Crowley* and *Potter* cited by Defendants are inapposite. In *Crowley*, the Court held that Amazon could not be liable because it "acted as no more than a second party to a communication" when it knowingly forwarded information to a credit card verification company. 166 F. Supp. 2d 1263, 1266 (N.D. Cal. 2001). In *Potter v. Havlicek*, the Court concluded that "computer software alone" is not a "device" because the ECPA "does not contemplate imposing civil liability on software manufacturers and distributors for the activities of third parties" in a case arising out of a nasty divorce where the victim of a jealous husband sued the husband for a Wiretap violation and the husband interpleaded the company that designed the software he used to spy on his spouse. 2008 WL 2556723 at *7 (S.D. Ohio June 23, 2008). Plaintiffs here allege seven devices, not computer software alone. More importantly, the Defendants are not arms-length software designers but instead the actual acquirers of the Plaintiffs' communications.

"designed to track and record an individual Internet user's communications … across the Internet." Compl. ¶ 41.

Criminal or Tortious Purpose – Defendants may be liable under the ECPA even if they have the consent of a party to the communication or are deemed a party to the communication where "such communication is intercepted [i.e. acquired] for the purpose of committing any criminal or tortious act in violation of … the laws of the United States or of any State." 18 U.S.C. § 2511(2)(d). In *Sussman v. ABC*, the Ninth Circuit explained this statutory exception to the consent and party exceptions applies where the underlying act is criminal or tortious for reasons unrelated to the means by which it was carried out. 186 F.3d 1200 (9th Cir. 1999). "Under §2511, the focus is not upon whether the interception violated another law; it is upon whether the purpose for the interception – *its intended use* – was criminal or tortious. … Where the taping is legal, but is done for the purpose of facilitating some further impropriety … section 2511 applies." *Id*. at 1202.

In this case, the precise method by which Facebook acquired and the health care Defendants disclosed PII is not the entire harm. Suppose Defendants had carried out this scheme without the use of the Internet – rather than disclosing PII via cookies, IP addresses, and device identifiers, the health care Defendants mailed Facebook a hard-copy database of every person with whom they exchanged off-line communications regarding medical conditions, services, or providers.[24] After receiving this information off-line, Facebook uses it for advertising. As they do in this case, the plaintiffs in such a situation would have actionable claims, and the defendants' conduct would violate several other medical privacy laws. Here, it is not just that Defendants schemed to acquire and disclose the Plaintiffs' communications in real-time without authorization. The nature of the information exchanged makes it tortious because the unauthorized acquisition and disclosure of sensitive health information is criminal and tortious – regardless of the technology employed.

3. Plaintiffs State a Claim Under the California Invasion of Privacy Act

CIPA § 631 – Plaintiffs re-state the arguments made for the federal Wiretap claim regarding

[24] This hypothetical is not far-fetched. *See* http://adage.com/article/datadriven-marketing/marketers-board-offline-online-data-train/293220/ (describing how Facebook and other companies are working to "turn[] offline consumer data into a tool for digital marketing.").

"content," Facebook's status as a "third-party" cookie company outside the Wiretap Act's exception for parties to a communication, and "device." In addition, Plaintiffs point this Court to the actual text of CIPA, which does not require a "device" but instead prohibits interceptions "by means of any machine, instrument, or contrivance, *or in any other manner*" (emphasis added). Like the federal Act, CIPA focuses on function, not static form.

CIPA § 632 – Plaintiffs plead CIPA section 632 in the alternative. If Facebook is deemed a party to the communication even though it is admittedly a "third-party cookie" company, CIPA section 632 also forbids recording a conversation where "a party to [the] conversation has an objectively reasonable expectation of privacy that the conversation is not being overheard or recorded," *Flanagan v. Flanagan*, 27 Cal. 4th 766, 777 (2002). As Facebook duly notes, California courts have held that Internet communications cannot be considered confidential in some circumstances. Mot. to Dismiss 23:15-17. However, no California court has held that an Internet communication is not confidential when one of the parties to the communication explicitly promises that it will not be disclosed to a third-party. In *Nickelodeon*, the Third Circuit ruled that a website's privacy promises may "create[] an expectation of privacy" on those websites. No. 15-1441, 2016 WL 3513782, at *22 (3d Cir. June 27, 2016). In this case, the health care Defendants not only "created an expectation of privacy" by their very promises but that expectation was made all the more reasonable by the fact that the health care Defendants are HIPAA-covered entities or otherwise trusted health care organizations, and that "[o]ne can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health[.]" *Norman-Bloodsaw*, 135 F.3d at 1269. Facebook's assertion that CIPA "was intended to apply to traditional recording mechanisms" and not Internet technology flies in the face of California courts' consistent modernizing of CIPA. *See In re: Google Inc. Gmail Litig.*, 2013 WL 5423918 at *21 (N.D. Cal. 2013) (noting California Supreme Court has consistently interpreted CIPA broadly and "regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme.").

Pre-emption – The Wiretap Act does not pre-empt CIPA or other state laws (including common law claims) designed to protect privacy. *See Shively v. Carrier IQ*, No. C-11-5775 EMC,

2012 WL 3026553, at *3-5 (N.D. Cal. July 24, 2012); *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal. 2011); *In re: NSA Telcomms. Records Litig.*, 483 F. Supp. 2d 934, 939 (N.D. Cal. 2007); *Leong v. Carrier IQ*, No. 12-01562 GAF (MRWx), 2012 WL 1463313 (C.D. Cal. Apr. 27, 2012); *Lane v. CBS Broad., Inc*., 612 F. Supp. 2d 623, 637 (E.D. Pa. 2009); *People v. Conklin*, 12 Cal. 3d 259 (1974); *Kearney v. Solomon Smith Barney, Inc*., 39 Cal. 4th 95 (2006). "Complete preemption … arises only in 'extraordinary' situations. The test is whether Congress clearly manifested an intent to convert state law claims into federal-question claims." *Ansley v. Ameriquest Mortg. Co*., 340 F.3d 858, 862 (9th Cir. 2003).

In *Shively v. Carrier IQ*, Judge Chen noted "*Bunnell* is fundamentally flawed because it fails to take into account the legislative history[.]" *Shively*, No. C-11-5775 EMC, 2012 WL 3026553 at *5. The legislative history to the Wiretap Act makes clear that Congress did not intend to supplant state law. *See* S. Rep. No. 90-1097, at 2187 (1968) ("The proposed provision envisions that *States would be free to adopt more restrictive legislation*, or no legislation at all, but not less restrictive legislation."); S. Rep. 99-541, at 3589 (1986) ("[T]he states must enact statutes which are *at least as restrictive* as the provisions of chapter 119 before they can authorize their state courts to issue interception orders."). "Rather than leaving no room for supplementary state regulation, Congress expressly authorized states to legislate in this field. Congress apparently wanted to ensure that states meet baseline standards, however, and thus federal law supersedes to the extent that state laws offer less protection than their federal counterparts." *Shively*, No. C-11-5775 EMC, 2012 WL 3026553 at *7. *Bunnell* and *Google Street View*, the two cases cited by Defendants, "are, by far, in the minority." *Leong*, No. 12-01562 GAF (MRWx), 2012 WL 1463313 at *3.

In addition, Defendants' misstate the nature of Plaintiffs' claims by arguing "each of plaintiffs' state-law claims is based on an alleged interception of electronic communications[.]" Mot. to Dismiss 24:9-10. As explained above, Plaintiffs would have a claim for damages even if the Defendants' scheme did not involve electronic communications. Moreover, to Plaintiffs' knowledge, no court has ever held that the federal Wiretap Act pre-empts traditional common law claims that pre-dated the Act's creation in 1968. *See In re: Google Street View*, 794 F. Supp. 2d 1067, 1085-86 (N.D. Cal. 2011) (Wiretap does not pre-empt non-CIPA cause-of-action).

Extra-territoriality – There's nothing extra-territorial about CIPA's application to this case. Facebook (1) is a California company that (2) directs its Internet tracking activities from California, (3) receives tracked Internet communications in California, (4) includes a binding Terms of Use adopting California law to govern all disputes with its members, and (5) upon information and belief, requires web-developers utilizing Facebook source code to also adopt California law. Compl. ¶ 306. Thus, a substantial portion of the challenged conduct (including that of the health care Defendants) occurred in California by virtue of Facebook's activities here and the health care Defendants have consented to the application of California law to govern its relationship with Facebook. *Id.* at ¶ 306e.

Moreover, CIPA's plain language applies to out-of-state wiretappers "who aid, agree[] with, employ[], or conspire[] with any person to … permit, or cause to be done any of the acts" prohibited by CIPA. Cal. Penal Code § 631(a). Those prohibited acts are as follows:

> Any person who … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, *or received at any place within this state*; or *who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained* ….

Plaintiffs have adequately alleged that Facebook received the information in California and that Facebook directs its tracking activities in California. Compl. ¶ 306b-c. CIPA applies.

4. Plaintiffs State Claims for California Constitutional Invasion of Privacy and Intrusion Upon Seclusion

Invasion of Privacy – As described by the California Supreme Court, the purpose of California's constitutional invasion of privacy tort "is readily discernible" as the initiatives text warned of "unnecessary information gathering by public and private entities – [such as] computer stored and generated dossiers and cradle-to-grave profiles on every American." *Hill v. NCAA*, 7 Cal. 4th 1, 15 (1994). "The evil addressed is … business conduct in collecting and stockpiling information … [and] [t]he Privacy Initiative's primary purpose is to afford some individuals some measure of protection against this most modern threat to personal privacy." *Id.* at 21. A California invasion of privacy claim is "not so much one of total secrecy as it is of the right to define one's

circle of intimacy – to choose who shall see beneath the quotidian mask." *Id.* at 25. Invasion of privacy has three elements: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Id.* at 39-40. Plaintiffs have adequately alleged all three elements.

Plaintiffs alleged "legally protected privacy interests" in the form of (a) the ECPA's Wiretap and Pen Register provisions;[25] (b) the Computer Fraud and Abuse Act and its state corollaries; (c) CIPA; (d) HIPAA; (e) Cal. Civ. Code § 1798.91; and (e) the privacy promises of the health care Defendants. Compl. ¶ 325. Plaintiffs alleged reasonable expectations of privacy[26] through these legally protected privacy interests and the health care Defendants' privacy promises. *See Riley*, 134 S. Ct. at 2473 (Data contained on smartphone, include visits to WebMD); *Norman-Bloodsaw*, 135 F.3d at 1260 (medical information); *In re: Nickelodeon*, 2016 WL 3513782 (violation of Internet privacy promises); *In re: Google Cookie Placement*, 806 F.3d at 150 (violation of Internet privacy promises); *Opperman*, 87 F. Supp. 3d 1018, 1059 (contact lists); *Lawlor v. North American Corp. of Ill.*, 983 N.E.2d 414, 426 (Ill. 2012) (phone records). Finally, Plaintiffs alleged serious invasions of privacy that constitute an egregious breach of social norms. *In re: Google Cookie Placement*, 806 F.3d at 150 (obtaining information through "deceit and disregard."); *In re: Nickelodeon*, 2016 WL 3513782 (3d Cir. June 27, 2016) (collecting information through dubious tactics); *Opperman* 87 F. Supp. 3d at 1061 ("Surreptitious theft of personal contact information … has [not] come to [be] qualified as 'routine commercial behavior.'"); *Campbell v. Facebook*, 77 F. Supp. 3d 836 (N.D. Cal. 2014) (analyzing Wiretap claim, "The court rejects the suggestion that any activity that generates revenue for a company should be considered within the 'ordinary course of business.'").

[25] The Pen Register Act prohibits non-consensual use of a "pen register" to track "dialing, routing, addressing, or signaling information" without consent. 18 U.S.C. § 3121, *et seq.* Thus, even if this Court finds that the URLs alleged do not contain content, Plaintiffs still have a legally protected privacy interest in DRAS.

[26] Through the Pen Register Act, plaintiffs distinguish between a reasonable expectation of privacy against disclosure of information to the government versus a reasonable expectation against disclosure to a private entity. Under the Pen Register Act, American consumers have a reasonable expectation of privacy that a private party cannot install a pen register or trap and trace device without their consent or an exception authorized by the Act. 18 U.S.C. § 3121, *et seq.* As detailed herein, Defendant Facebook has publicly referred to warrantless collection of mere IP addresses by government agents as raising "civil liberties and human rights concerns."

Intrusion Upon Seclusion – "Intrusion upon seclusion" is similar but distinct from invasion of privacy. To make a claim for intrusion, a plaintiff must allege an intrusion into a private matter, including "some zone of … privacy surrounding, or obtain[ing] unwanted access to data about the plaintiff … [and] an objectively reasonable expectation" of privacy in "the place, conversation, or data source." *Shulman v. Group W. Prods., Inc*., 18 Cal. 4th 200, 232 (1998). In this case, Plaintiffs allege objectively reasonable expectations of privacy based upon federal and state statutes as well as the explicit promises made by the health care Defendants with which they were communicating.

Second, the plaintiff must allege that the intrusion is "highly offensive" to a reasonable person. For both intrusion and invasion of privacy, "highly offensive" or "serious" is ultimately a jury question, but first a court must determine "whether, as a matter of policy, such conduct should be considered, as a matter of law, not highly offensive." *Taus v. Loftus*, 40 Cal. 4th 683, 737 (2007). Congress and every state has already made this "policy" decision through the passage of criminal and civil laws designed to protect communications and health care privacy. Violation of the ECPA or CFAA subjects a defendant to imprisonment. Violation of HIPAA subjects covered entities to substantial fines and other civil penalties. Beyond criminal penalties, California explicitly declared that the activities in this case are a "serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630. Further, the California Supreme Court explicitly held that "eavesdropping [or] wiretapping" gives rise to the tort of intrusion upon seclusion. *Shulman* at 863, 868. Because this case involves the unauthorized tracking and disclosure of sensitive medical information protected by the Constitution, common law, statutes, and regulations, a reasonable jury could find the intrusions "highly offensive" or "serious."

5. The Claim for Negligence Per Se Is Valid

A presumption of negligence is created when four elements are established: (1) [the defendant] violated a statute, ordinance, or regulation of a public entity; (2) the violation proximately caused death or injury to person or property; (3) the injury resulted from an occurrence of the nature which the statute, ordinance, or regulation was designed to prevent; and (4) the person suffering the injury to his person or property was one of the class of persons for whose protection the statute, ordinance, or regulation was adopted. Cal. Evid. Code § 669(a); *Quiroz v. Seventh Ave.*

Ctr., 140 Cal. App. 4th 1256, 1285 (2006) (citing same).

Plaintiffs allege that Defendants' conduct violated HIPAA, which is a statute of a public entity, and that the violation proximately caused them injury. HIPAA was enacted to prevent unauthorized use of personally identifiable health information, and protects individuals to whom health information relates. To de-identify health information, HIPAA requires removal of the names "of the individual or of the relatives, employers, or household members of the individual." 45 C.F.R. § 164.514(b)(2)(i)(A). IP addresses must also be removed. 45 C.F.R. § 164.514(b)(2)(i)(O). As alleged, the information transmitted to Facebook, which contained health information, was not de-identified. As individuals seeking information about their own health conditions or those of a household member, each Plaintiff falls into the class of persons HIPAA aims to protect.

Defendants' violation of the statute proximately caused Plaintiffs injury – namely, the violation of their rights to privacy in their health information. The violation of this right is precisely the type of occurrence that HIPAA was enacted to prevent. Therefore, Plaintiffs have alleged all elements of a negligence claim under a negligence per se theory.

While there is an economic component to the injury alleged by Plaintiffs (namely, the value of their data), the loss that Plaintiffs allege is not strictly economic. HIPAA conferred upon the health care Defendants that are covered entities a duty to keep Plaintiffs' health information private. As a result of the health care Defendants' breach of this duty, Plaintiffs' privacy rights were violated causing them harm and Defendants liable for that damage.

6. <u>The Claim For Negligent Disclosure of Confidential Information Is Valid</u>

Even non-health care websites have a legal obligation to keep the privacy promises they make. *See In re: Nickelodeon,* 2016 WL 3513782 ("Viacom created an expectation of privacy on its websites and then obtained the plaintiffs' personal information under false pretenses."). In this case, the health care Defendants explicitly promised not to disclose the plaintiffs' PII and communications to third-parties, with limited exceptions that do not apply here. And then they did so anyway. Like Viacom, they helped create the expectation and a duty to keep their promise, then they breached it.

Defendants' argument about referer headers and public URLs obfuscates the facts of this case. As discussed at length above, and set forth in the Complaint, the disclosures also included PII connected to sensitive health communications. Defendants argue that because public URLs are not protected health information, HIPAA's restrictions are irrelevant. Again, Defendants distort the facts. Plaintiffs have not alleged that use of anonymous URLs violates HIPAA. Instead, this case is about sensitive communications attached to PII. In these exchanges, Facebook acquires not only information sufficient to identify the visitor, but also content pertinent to his or her health condition. As discussed above, the Ninth Circuit has held that URLs contain "content" when they include search terms or similar communications made by the user. *In re: Zynga*, 750 F.3d at 1109. For example, the text following ".org" in the URL that Plaintiff Jane Doe II visited, http://my.clevelandclinig.org/search/results?q=intestine%20transplant (Compl. ¶ 188), would constitute "content."

As is required to assert a negligence claim under California law, Plaintiffs alleged "appreciable, nonspeculative, present harm." *In re: Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 962 (S.D. Cal. 2012) (citing *Aas v. Superior Court*, 24 Cal. 4th 627, 646 (2000)); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009), aff'd, 380 Fed.Appx. 689 (9th Cir. 2010)). This harm need not be tangible. Plaintiffs were personally harmed when their sensitive medical information was disclosed to, tracked, and intercepted by Facebook without their knowledge or consent, rendering their information no longer private. To call into question whether such an invasion of Plaintiffs' privacy constitutes sufficient harm is to question whether the privacy of one's health information has value at all. If health information were worthless, statutes such as HIPAA would serve no purpose. The very existence of numerous federal and state laws protecting individuals' privacy demonstrates widespread recognition that privacy, particularly of sensitive medical information, is inherently valuable. Because the right to privacy in certain information is intrinsically valuable, the loss of such privacy through improper disclosure causes actual harm.

Further, Plaintiffs' allegations of actual harm distinguish their case from *In re Sony* and *Regents of Univ. of Cal. v. Superior Court*, where the plaintiffs did not allege that the data at issue

had been misused. 903 F. Supp. 2d at 962-63 (dismissing negligence claim where plaintiffs alleged exposure to increased identity theft and fraud risks); 220 Cal. App. 4th 549 (2013) (dismissing claim for negligent disclosure of information where plaintiffs could not allege misuse of same).

7. The Claim for Breach of Fiduciary Duty of Confidentiality Survives

Establishing the tort for violation of a fiduciary duty requires: (1) a breach; (2) of a fiduciary duty; and (3) that the plaintiff suffered damages proximately caused by defendant's conduct. Restatement (Second) of Torts, § 874 (1979). The comment to Restatement (Second) of Torts § 874 explains:

> *A fiduciary relation exists between two persons when one of them is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation* . . . the beneficiary is entitled to tort damages for harm caused by the breach of duty arising from the relation. … In addition to or in substitution for these damages the beneficiary may be entitled to restitutionary recovery, since not only is he entitled to recover for any harm done to his legally protected interests by the wrongful conduct of the fiduciary, but ordinarily he is entitled to profits that result to the fiduciary from his breach of duty and to be the beneficiary of a constructive trust in the profits. . . . A person who knowingly assists a fiduciary in committing a breach of trust is himself guilty of tortious conduct and is subject to liability for the harm thereby caused.

Restatement (Second) of Torts § 874, cmts. (a)-(c) (emphasis added). One breach of fiduciary duty commonly regarded as giving rise to an action in tort is the disclosure of confidential information. *See, e.g., Horne v. Patton*, 287 So. 2d 824 (Ala. 1973); *Cannell v. Medical & Surgical Clinic*, 315 N.E.2d 278 (Ill. App. Ct. 1974); *Felis v. Greenberg*, 273 N.Y.S.2d 288 (N.Y. Sup. Ct. 1966); *Doe v. Roe*, 400 N.Y.S.2d 668 (N.Y. Sup. Ct. 1977); *Schaffer v. Spicer*, 215 N.W.2d 134 (S.D. 1974). The Northern District of California has opined on the importance of a "confidential relationship" in the context of a fiduciary duty:

> A "confidential relationship" arises only "where a confidence is reposed by one person in the integrity of another, and . . . the party in whom the confidence is reposed . . . voluntarily accepts or assumes to accept the confidence." Significantly, in the context of claims for breach of fiduciary duty . . . '[t]he essence of a fiduciary or confidential relationship is that the parties do not deal on equal terms, because the person in whom trust and confidence is reposed and who accepts that trust and confidence is in a superior position to exert unique influence over the dependent party.

City Sols., Inc. v. Clear Channel Commc'ns, Inc., 201 F. Supp. 2d 1048, 1050-51 (N.D. Cal. 2002) (citing *Barbara A. v. John G.*, 145 Cal. App. 3d 369, 382–83 (1983); *Vai v. Bank of America*, 56

Cal. 2d 329, 338 (1961) ("The key factor in the existence of a fiduciary relationship lies in control by a person over the property of another")).

Here, Plaintiffs placed their confidence in Defendants that Plaintiffs' confidential medical data and communications with Defendants' websites regarding their medical conditions would be kept private. Defendants' complete control over Plaintiffs' information, as alleged in the Complaint, demonstrates a relationship that is not on equal footing. Despite this inequality, which strongly suggests a confidential relationship that creates a duty, Defendants argue that their privacy policies do not guarantee any privacy of Plaintiffs' information. But, the very titles of these "privacy policies" belie Defendants' argument, as they would have this Court believe that what they actually have are not "privacy policies" but "lack of privacy policies." Regardless of Defendants' assertions to the contrary, the privacy policies and confidential relationships between the parties create a duty.

Defendants do not challenge the breach requirement in section 874, so there is no need to address this point. Finally, as to damages, the comment to section 874 quoted *supra* provides a clear measure for damages. *See* Restatement (Second) of Torts, §§ 874, 875 ("Each of two or more persons whose tortious conduct is a legal cause of a single and indivisible harm to the injured party is subject to liability to the injured party for the entire harm."), 876 ("[H]arm resulting to a third person from the tortious conduct of another, one is subject to liability . . . ."); *see also*, Restatement (Second) of Torts § 874, cmt. (c) (liability for breach of fiduciary duty applies to both breaching party and any other party acting in concert). Accordingly, this claim should proceed.

Finally, amongst other damages, Plaintiffs are "entitled to profits that result to the fiduciary from his breach of duty." Even if the health care Defendants do not directly profit from pilfering Plaintiffs' information and selling it to Facebook (not alleged in the Complaint), all Defendants are still liable to Plaintiffs because Facebook profited from the information, as collecting/selling personal information is an inherent part of its business model, as set out above.

8. <u>The Breach of Duty of Good Faith and Fair Dealing Is Proper</u>

Plaintiffs' have adequately stated a Good Faith and Fair Dealing claim against Facebook. Citing only *Partti v. Palo Alto Med. Found. for Health Care, Research & Educ., Inc.*, 2015 WL 6664477 (N.D. Cal. Nov. 2, 2015), Facebook ignores the full quote therefrom, choosing instead

selective words from the holding. Mot. to Dismiss 32:23-25. The full quote reads: "If the allegations do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of action**,** they may be disregarded as superfluous as no additional claim is actually stated." (citing *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1394, as modified on denial of reh'g (2001)). Here Plaintiffs allege a breach and seek relief different and independent from relief claimed under other counts. Furthermore, there is no companion contract cause of action in the Complaint. In the Order Granting Summary Judgment in *Partti*, Judge Grewal held, "In order for Defendants to have breached the implied covenant, there must be a contract to breach." *Partti* at 10. Here, there is a contract, an implied duty, and a breach.

9. The Fraud Claim Is Proper

To state an action for fraud, a plaintiff must plead with specificity an intentional misrepresentation of material fact with knowledge of its falsity and intent to induce reliance, actual reliance, and damages proximately caused by the reliance. *Gonsalves v. Hodgson*, 38 Cal. 2d 91, 100-02 (1951). Plaintiffs' actual and constructive fraud claims satisfy Rule 9(b)'s specificity requirement. Plaintiffs allege the "who" (Facebook and its employees, along with the health care Defendants), the "what" (surreptitious tracking and interception of private health-related communications), the "when" (during the class period), the "where" (in the interactions between Plaintiffs' computers, health care Defendants' websites, and Facebook's servers) and the "how" (through specifically identified, improperly planted cookies that track and intercept communications). Having falsely promised that they would only share health-related information in limited circumstances, the Defendants were duty-bound to protect this information from improper tracking and interception.

Defendants argue that Facebook made no misrepresentation – essentially, that Plaintiffs were aware of and consented to the improper tracking and interception. This argument is without merit, as discussed above. Plaintiffs alleged intent to deceive, reliance, and damages arising therefrom, which satisfies the elements set forth in *Gonsalves*. 38 Cal. 2d 91.

10. The Quantum Meruit Claims Were Properly Alleged

The Complaint includes sufficient allegations to support a claim of quantum meruit. "The underlying idea behind quantum meruit is the law's distaste for unjust enrichment. If one has received a benefit which one may not justly retain, one should 'restore the aggrieved party to his [or her] former position by return of the thing *or its equivalent* in money." *Maglica v. Maglica*, 66 Cal. App. 4th 442, 449 (1992) (emphasis added) (internal citations omitted). Should Plaintiffs be unable to prove a binding contract between Facebook and them, or elect to rescind it, they are not without remedy. Plaintiffs' sensitive medical information was collected for the purpose of direct marketing. Compl. ¶ 370. Facebook cannot justly retain the benefit it obtained (Compl. ¶ 80) from violating Plaintiffs' privacy rights (Compl. ¶ 371). Plaintiffs would therefore be entitled to compensation for the value of their personally identifiable health-related information pursuant to quantum meruit.

V. CONCLUSION

For the foregoing facts and reasons, the Motion should be denied in its entirety and Defendants ordered to Answer. If the Motion is granted, either in whole or in part, Plaintiffs hereby request leave to amend.

DATED: August 1, 2016

KIESEL LAW LLP

By: */s/ Jeffrey A. Koncius*
Paul R. Kiesel
Jeffrey A. Koncius
Nicole Ramirez

THE GORNY LAW FIRM, LC
Stephen M. Gorny [Admitted *Pro Hac Vice*]
steve@gornylawfirm.com
Chris Dandurand [Admitted *Pro Hac Vice*]
chris@gornylawfirm.com
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

BARNES & ASSOCIATES

Jay Barnes [Admitted *Pro Hac Vice*]
jaybarnes5@zoho.com
Rod Chapel [Admitted *Pro Hac Vice*]
rod.chapel@gmail.com
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

EICHEN CRUTCHLOW ZASLOW & McELROY

Barry. R. Eichen [Admitted *Pro Hac Vice*]
beichen@njadvocates.com
Evan J. Rosenberg [Admitted *Pro Hac Vice*]
erosenberg@njadvocates.com
Ashley A. Smith [Admitted *Pro Hac Vice*]
asmith@njadvocates.com
40 Ethel Road
Edison, NJ 08817
Tel.: 732-777-0100
Fax: 732-248-8273

THE SIMON LAW FIRM, P.C.

Amy Gunn [Admitted *Pro Hac Vice*]
agunn@simonlawpc.com
800 Market St., Ste. 1700
St. Louis, MO 63101
Tel.: 314-241-2929
Fax: 314-241-2029

BERGMANIS LAW FIRM, L.L.C.

Andrew Lyskowski [to be admitted *Pro Hac Vice*]
alyskowski@ozarklawcenter.com
380 W. Hwy. 54, Ste. 201
Camdenton, MO 65020
Tel.: 573-346-2111
Fax: 573-346-5885